CLAIMS

What is claimed is:

1. A system for authentication of a counterfeit-resistant document, comprising:

(a) means for automatically describing an apparently non-deterministic characteristic of a recording medium of the document,

(b) means for receiving a document content of the counterfeit resistant document;

(c) means for storing the description of the apparently non-deterministic characteristic and document content in association with each other; and

(d) means for comparing the stored description of the apparently non-deterministic characteristic and document content with an observed apparently non-deterministic characteristic and document characteristic.

2. The system according to claim 1, wherein the said non-deterministic characteristic comprises a feature that is incompletely represented in a tri color representation.

3. The system according to claim 1, wherein said apparently non-deterministic characteristic comprises a stenangiographic code.

4. The system according to claim 1, wherein said description of said apparently non-deterministic characteristic is imprinted on the document.

5. The system according to claim 1, wherein said description of said apparently non-deterministic characteristic and said document content are imprinted as encrypted data on said document.

6. The system according to claim 5, wherein said encryption comprises a public key-private key algorithm.

7. The system according to claim 1, wherein said document comprises a digital notary signature to identify alterations.

8. The system according to claim 1, further comprising network print driver software, transmitting an identification of said recording medium and a description of the document content to a remote server upon printing of said document content on said medium.

9. The system according to claim 1, further comprising network print driver software, for transmitting an identifier of said recording medium to a remote server, receiving a description of said apparently non-deterministic characteristic from the remote server, and imprinting an encrypted message on said medium comprising a description of said apparently non-deterministic characteristic and said document content or a digital signature thereof.

10. The system according to claim 1, wherein said automatic description means comprises an optical imaging system.

11. The system according to claim 1, wherein the automatic document content receiving means comprises means for receiving an electronic page description language file.

12. The system according to claim 1, wherein said comparing means comprises an optical imager.

13. The system according to claim 1, further comprising a financial accounting record, to account for at least a portion of a verification procedure.

14. The system according to claim 1, further comprising a financial accounting record, to account for a database lookup process.

15. The system according to claim 1, wherein said comparing means is adapted to compare at least two descriptions of apparently non-deterministic characteristics of the same medium having differing degrees of complexity.

16. The system according to claim 15, wherein an accounting system selectively accounts for a different fee for comparing each of said at least two descriptions of apparently non-deterministic characteristics.

17. The system according to claim 1, further comprising a financial accounting record, selectively and differentially accounting for comparing operations based on a decision dependent thereon.

18. The system according to claim 1, wherein the characteristic is integral with said recording media.

19. The system according to claim 1, wherein the characteristic is provided as an imprinted feature of the recording media, generated in a distinct process from the recording of the document content.

20. The system according to claim 1, wherein the indicia is imprinted on the recording media in a consolidated process with an imprinting of the document content.

21. The system according to claim 1, wherein the document further comprises an identifier, and wherein the apparently non-deterministic characteristic and document content are stored in reference to said identifier.

22. The system according to claim 21, wherein said identifier is a serial number.

23. The system according to claim 21, further comprising a human user interface for manually entering the identifier.

24. The system according to claim 21, wherein said identifier is a machine readable code, further comprising an identifier reading system.

25. The system according to claim 1, wherein said means for receiving a document description comprises an optical scanner.

26. The system according to claim 1, wherein said automatic describing means and said receiving means employ a common imaging subsystem.

27. The system according to claim 1, wherein said means for automatic describing means comprises an optical spectrographic analyzer, selectively analyzing narrowband spectral characteristics.

28. The system according to claim 1, wherein said apparently non-deterministic characteristic comprises at least one region having a selectively defined magnetic property.

29. The system according to claim 1, wherein said an apparently non-deterministic characteristic is an indicia printed with MICR toner.

30. The system according to claim 1, wherein said comparing means provides an adaptive threshold comparison for authenticating.

31. The system according to claim 1, wherein said comparing means applies fuzzy logic for authentication.

32. The system according to claim 1, wherein said comparing means applies a transform to a scanned image of the document and performs a comparison in a transformed domain or in a normalized space.

33. The system according to claim 32, wherein said transform is rotationally invariant two dimensional transform.

34. The system according to claim 1, wherein said comparing means applies a transform to an image of the document to normalize for a characteristic selected from the group consisting of rotation, skew, stretch, and fade.

35. The system according to claim 1, wherein said storing means stores the document content in encrypted form.

36. The system according to claim 1, wherein said apparently non-deterministic characteristic indicia and said document content are stored in separate fields of a database.

37. The system according to claim 1, wherein said document has a plaintext decryption key imprinted thereon, said document content being stored remotely, further comprising means for transmitting in encrypted form the description of the apparently non-deterministic characteristic and document content, for decryption by the decryption key

38. The system according to claim 1, further comprising a reader device, comprising a document scanner for acquiring a document content, and a characteristic reader for determining the apparently non-deterministic characteristic.

39. The system according to claim 38, wherein said reader device is remote from a storage medium repository associated with said storing means, wherein said reader device further comprises a telecommunication subsystem for communicating with said storing means.

40. The system according to claim 1, wherein said document comprises self-authenticating features.

41. The system according to claim 1, wherein said document comprises a self-authenticating digital signature.

42. The system according to claim 1, further comprising a reader device, comprising a characteristic reader for determining the characteristic, and a self-contained authentication processor operating on data derived directly and concurrently from the document.

43. The system according to claim 1, wherein the document further comprises self-authenticating features comprising an encrypted representation of the content, said system further comprising a secure cryptographic processor associated with said means for comparing.

44. The system according to claim 43, wherein the cryptographic processor decrypts representations of both said document content and said apparently non-deterministic characteristic.

45. The system according to claim 1, wherein the characteristic comprises a stochastic characteristic integral with the recording media, wherein the characteristic is analyzed to provide an encryption key necessary for an authentication process.

46. The system according to claim 45, wherein the extracted characteristic is processed in a local authentication device for self-authentication of said document.

47. The system according to claim 45, wherein said characteristic corresponds to a private key of a public key-private key cryptographic algorithm.

48. The system according to claim 47, wherein a unique identifier of said document is transmitted to a remote processor, a representation of the document content encrypted using a public key-private key algorithm and information defining an appropriate public key is transmitted to a local cryptographic processor, and said local cryptographic processor decrypts the document based on the encrypted document content, public key and private key.

49. The system according to claim 1, wherein a unique identifier of said document comprises a serial number, the characteristic comprises a pseudorandom copy-resistant printed marking, wherein a secret algorithm defines a mapping between the serial number and a pattern

of the pseudorandom copy-resistant printed marking, wherein said system further comprises means for executing said secret algorithm and maintaining a security of said secret algorithm, and means for comparing an observed characteristic of a document to be authenticated to an output of said executing means.

50. A method for authentication of a counterfeit resistant document, comprising the steps of:

(a) automatically describing an apparently non-deterministic characteristic of a recording medium of the document

(b) receiving a document content of the counterfeit resistant document;

(c) storing the description of the apparently non-deterministic characteristic and document content in association with each other; and

(d) comparing the stored description of the apparently non-deterministic characteristic and document content with an observed apparently non-deterministic characteristic and document characteristic.

51. The method according to claim 50, wherein the apparently non-deterministic characteristic is incompletely represented in an RGB color-space.

52. The method according to claim 50, further comprising the step of uniquely identifying the recording medium.

53. A method, comprising the steps of:

(a) providing a counterfeit resistant document recording medium, having thereon a predefined unique document identifier and at least one security feature;

(b) defining a variable document content for imprinting on an identified recording medium;

(c) storing the variable document content in a database indexed by associated document identifier; and

(d) authenticating the counterfeit resistant document by authenticating the security feature and comparing the stored document content with a perceived document content.

54. The method according to claim 53, wherein said authenticating the security feature comprises execution of a cryptographic process.

55. The method according to claim 53, further comprising the step of financially accounting for said storing.

56. The method according to claim 53, further comprising the step of financially accounting for said authenticating.

57. The method according to claim 53, wherein said authenticating step comprises a local process for authenticating the security feature and a remote process for authenticating the document content.

58. The method according to claim 57, wherein said remote process is asynchronous with and delayed from said local process.

59. A method for providing document security, comprising the steps of:

(a) providing a document to be authenticated, having predefined document content;

(b) providing a serialized piece of paper currency;

(c) physically associating the document and the paper currency;

(d) storing document content in association with the serial number of the paper currency.

60. The method according to claim 59, further comprising the step of authenticating the document by recalling a database record including a serial number of a piece of physically associated paper currency and a document content, analyzing the paper currency for identity of serialization and authenticity, and comparing the recalled document content with a document content of the document to be authenticated.

61. An authentication system comprising:

(a) a plurality of media, each having a plurality of counterfeit-resistant non-deterministic elements;

(b) a detector, detecting said elements;

(c) a storage system for storing a description of said detected elements;

(d) a recording system for recording a content on said medium;

(e) means for storing said content; and

(f) means for comparing a set of detected elements and stored content with a set of observed elements of the media and content to authenticate the media and content.

62. The system according to claim 61, wherein the elements comprise a non-deterministic directional vector of a characteristic of a respective element.

63. The system according to claim 61, wherein the elements are disposed in a non-deterministic spatial arrangement in said medium.

64. The system according to claim 61, wherein said stored description of said detected elements comprises an encrypted message generated by a process comprising irreversible compression of said description of said detected elements.

65. The system according to claim 64, wherein an encrypted message is separately defined for each of a plurality of regions of one of said media.

66. The system according to claim 61, wherein said means for comparing determines a correspondence and an associated reliability thereof, between said set of detected elements and stored content with a set of observed elements of the media and content.

67. The system according to claim 61, wherein the plurality of elements comprise fibers exhibiting dichroism, said description comprising a dichroism thereof.

68. The system according to claim 61, wherein the media comprises paper.

69. An authentication system comprising:

(a) an authentication certificate having a counterfeit resistant element and a document content;

(b) a secure code associated with the authentication certificate defining an apparently non-deterministic characteristic of the counterfeit resistant element and a digital signature of the document content;

(c) an system for reading the apparently non-deterministic characteristic; and

(d) a processor for comparing the read apparently non-deterministic characteristic of the authentication certificate and content thereof with the associated secure code to determine an authenticity of the authentication certificate, the authenticity being associated with a reliability thereof, based on:

stochastic variations in the apparently non-deterministic characteristic, and

stochastic variations in the received input used for generation of the associated secure code.

70. The system according to claim 69, wherein the secure code is a public-key/private-key authentication code.

71. The system according to claim 69, wherein the apparently non-deterministic characteristic comprises one or more characteristics selected from the group consisting of: a pseudorandom imprint pattern, a non-deterministic pattern of elements comprising the media, an interaction of an aliquot of liquid dye with non-deterministic pattern of elements comprising the media media, and a non-deterministic pattern of an imprint on the medium.

72. A method of authenticating a document, comprising:

providing a document stock having anti-counterfeit features;

preprinting the document with an essentially unique identifier;

defining a content for the document having an associated digital signature for verification of the document content and essentially unique identifier; and

printing the content on the document stock.

73. The method according to claim 72, further comprising the step of printing the digital signature on the document stock.

74. The method according to claim 73, further comprising the step of authenticating the document by verifying that the digital signature corresponds to the document content and essentially unique identifier.

75. The method according to claim 72, further comprising the step of receiving the digital signature and authenticating the document by verifying that the digital signature corresponds to the document content and essentially unique identifier.

76. The method according to claim 72, wherein the anticounterfeit features comprise a set of visually distinct fibers in said document stock.

77. The method according to claim 72, wherein the anticounterfeit features comprises a lithographed pattern printed on said document stock.

78. The method according to claim 72, wherein the essentially unique identifier comprises a composite of a random portion and a predictable portion.

79. The method according to claim 72, further comprising the step of accounting to a content proprietor for a printing of the document.

80. The method according to claim 79, wherein said accounting comprises issuing a request for the content and electronic payment information; and receiving content and associated digital signature.

81. The method according to claim 72, wherein said preprinting comprises printing with a printer having a non-secure communications channel.

82. The method according to claim 72, wherein said printing comprises printing with a printer having a non-secure communications channel.

83. The method according to claim 72, wherein said printing comprises communicating the essentially unique identifier over a network to a server, receiving the content over the network from the server, and printing the received content on the document stock.

84. The method according to claim 72, wherein said providing and preprinted are conducted securely.

85. The method according to claim 72, wherein the anticounterfeit features comprise at least one integral non-deterministic characteristic of the document stock.

86. The method according to claim 85, wherein the non-deterministic characteristic comprises a fiber pattern, further comprising the steps of recording the fiber pattern prior to said printing, and authenticating the document stock by comparing a consistency of the recorded fiber pattern with a fiber pattern determined at a time of authentication.

87. The method according to claim 72, further comprising the step of authenticating the document based on a public key-private key algorithm which authenticates the essentially unique identifier together with the document content.

88. An authenticatable recording medium, comprising:

a document stock having counterfeit resistant features;

an imprinted tamper resistant unique identifier on the document stock; and

a content recording surface.

89. The authenticatable recording medium according to claim 88, further comprising information content recorded on the content recording surface.

90. The authenticatable recording medium according to claim 89, further comprising a self-authenticating message recorded on the content recording surface for authenticating the information content and the tamper resistant unique identifier.

91. The authenticatable recording medium according to claim 88, further comprising an ascertainable integral non-deterministic characteristic of the document stock.

92. The authenticatable recording medium according to claim 91, wherein the non-deterministic characteristic comprises a fiber pattern.

93. The authenticatable recording medium according to claim 88, wherein the imprinted tamper resistant unique identifier comprises a predictable portion and a random portion.